UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/790,082	03/02/2004	Takeo Yoshida	118918	2490

25944 7590 05/09/2008

OLIFF & BERRIDGE, PLC
P.O. BOX 320850
ALEXANDRIA, VA 22320-4850

EXAMINER	
LOUIE, OSCAR A	

ART UNIT	PAPER NUMBER
2136	

MAIL DATE	DELIVERY MODE
05/09/2008	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/790,082	YOSHIDA, TAKEO	
	Examiner	Art Unit	
	OSCAR A. LOUIE	2136	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *22 January 2008*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-3,5-7 and 9-13* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-3, 5-7, and 9-13* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

This first non-final action is in response to the Request for Continued Examination filing of 01/22/2008. In light of the applicant's amendments, remarks, and with further consideration of the claim limitations, the examiner hereby withdraws his previous 35 U.S.C. 112 2nd paragraph rejections regarding Claims 1-3, 5-7, & 9-13. Claims 1-3, 5-7, & 9-13 are pending and has/have been considered as follows.

Claim Objections

1. Claims 1, 3, 5-7, 9, & 11 are objected to because of the following informalities:

- Claim 1 lines 6, 10, 15, 19, 22, 24, 29, & 32 recite the term "for" which should be "…configured to…";
- Claim 3 lines 1, 4, 8, & 11 recite the term "for" which should be "…configured to…";
- Claim 5 lines 3 & 7 recite the term "for" which should be "…configured to…";
- Claim 6 lines 6, 7, 10, 14, 20, & 23 recite the term "for" which should be "…configured to…";
- Claim 7 lines 3, 6, & 10 recite the term "for" which should be "…configured to…";
- Claim 9 lines 3, 6, 10, & 14 recite the term "for" which should be "…configured to…";
- Claim 11 line 3 recites the term "for" which should be "…configured to…";

Appropriate correction is required.

Claim Rejections - 35 USC § 102

2. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

3. Claims 1, 3, 5, & 10-12 are rejected under 35 U.S.C. 102(e) as being anticipated by Lander (US-7350229-B1).

Claim 1:

Lander discloses a network connection system comprising,

- "a client apparatus" (i.e. "a client") [column 8 line 45];
- "a third unit for transmitting the second connection authentication information generated by the client apparatus to the authentication server together with the connection request" (i.e. "When the user signs onto the front-end server cluster 202, the central security process 222 transmits the user login data (e.g., username and password) to the policy server 204") [column 11 lines 11-14];
- "a fourth unit for receiving the connection server address from the authentication server" (i.e. "Once the user is authenticated and gains access to the enterprise network (or protected resources in the enterprise network), the user's web browser may display a menu from which a service may be chosen") [column 2 lines 21-24];

- "a fifth unit for preparing first connection authentication information based on the user identification information input into the client apparatus" (i.e. "The user may then be prompted to sign onto the application") [column 2 lines 32-33];
- "transmitting the first connection authentication information to the connection server address of the connection server" (i.e. "a second authentication process is executed to check the authenticity of the user") [column 2 lines 34-38];
- "an authentication server" (i.e. "front-end server") [column 8 line 45];
- "a retention unit for storing second connection authentication information generated by the connection server based on user identification information" (i.e. "memory 106, and at least one storage device") [column 8 line 47];
- "associating the second connection authentication information with a connection server address of the connection server" (i.e. "Each front-end server and each back-end server may store user identifiers and corresponding access privilege codes in their respective databases, rather than using a single central database to store such information") [column 3 lines 4-7];
- "a first unit for acquiring, from the client apparatus, second connection authentication information that is generated by the client apparatus based on user identification information input into the client apparatus" (i.e. "When the user signs onto the front-end server cluster 202, the central security process 222 transmits the user login data (e.g., username and password) to the policy server 204") [column 11 lines 11-14];

- "acquiring a client address of the client apparatus when the first unit receives a connection request from the client apparatus" (i.e. "An electronic device, such as a front-end server 102 receives a client request 116") [column 8 lines 44-45];
- "a second unit for transmitting the client address to the connection server address associated with the second connection authentication information acquired by the first unit" (i.e. "Once the user is authenticated and gains access to the enterprise network (or protected resources in the enterprise network), the user's web browser may display a menu from which a service may be chosen") [column 2 lines 21-24];
- "transmitting the connection server address to the client apparatus" (i.e. "Once the user is authenticated and gains access to the enterprise network (or protected resources in the enterprise network), the user's web browser may display a menu from which a service may be chosen") [column 2 lines 21-24];
- "a connection server" (i.e. "back-end content servers") [column 8 line 66];
- "a sixth unit for allowing the first connection authentication information to be received from the client address, the client address being received from the authentication server" (i.e. "The user may then be prompted to sign onto the application") [column 2 lines 32-33];
- "a seventh unit for performing itself an authentication process by using the first connection authentication information transmitted from the client address" (i.e. "a second authentication process is executed to check the authenticity of the user. This second authentication process on the back-end server") [column 2 lines 35-36].

Claim 3:

Lander discloses an authentication server for being connected to a plurality of client apparatuses and a plurality of connection servers comprising,

- "a retention unit for storing second connection authentication information generated based on user identification information" (i.e. "memory 106, and at least one storage device") [column 8 line 47];
- "associating each second connection authentication information with a connection server address of a corresponding connection server" (i.e. "Each front-end server and each back-end server may store user identifiers and corresponding access privilege codes in their respective databases, rather than using a single central database to store such information") [column 3 lines 4-7];
- "a first unit for acquiring the second connection authentication information from the client apparatus and a client address when the first unit receives a connection request from the client apparatus" (i.e. "When the user signs onto the front-end server cluster 202, the central security process 222 transmits the user login data (e.g., username and password) to the policy server 204") [column 11 lines 11-14];
- "a second unit for transmitting the acquired client address to the connection server address of the connection server associated with the acquired second connection authentication information" (i.e. "Once the user is authenticated and gains access to the enterprise network (or protected resources in the enterprise network), the user's web browser may display a menu from which a service may be chosen") [column 2 lines 21-24];

- "transmitting, independent of the connection server, the connection server address to the client apparatus which has transmitted the connection request" (i.e. "Once the user is authenticated and gains access to the enterprise network (or protected resources in the enterprise network), the user's web browser may display a menu from which a service may be chosen") [column 2 lines 21-24].

Claim 5:

Lander discloses a connection server operating with an authentication server and a client apparatus comprising,

- "a control unit for receiving a client address of the client apparatus from the authentication server after the authentication server authenticates information received from the client address" (i.e. "The user may then be prompted to sign onto the application") [column 2 lines 32-33];
- "allowing authentication information to be received from the client address" (i.e. "The user may then be prompted to sign onto the application") [column 2 lines 32-33];
- "an authentication unit for receiving the authentication information from the client apparatus having the client address to perform itself an authentication process by using the authentication information" (i.e. "a second authentication process is executed to check the authenticity of the user. This second authentication process on the back-end server") [column 2 lines 35-36].

Claim 10:

Lander discloses a connection server operating with a client apparatus and an authentication server comprising,

- "a control unit that receives from the authentication server an address of the client apparatus and allows communication from the address of the client apparatus for a predetermined period" (i.e. "The user may then be prompted to sign onto the application") [column 2 lines 32-33];
- "a transmitting unit that transmits to the authentication server information indicating that the connection server has shifted to a connection wait state in which the connection server allows communication from the address of the client apparatus for the predetermined period" (i.e. "The user may then be prompted to sign onto the application") [column 2 lines 32-33].

Claim 11:

Lander discloses a network connection system comprising,

- "a client apparatus" (i.e. "a client") [column 8 line 45];
- "calculates first authentication information unique to the client apparatus to register the first authentication information in the connection server" (i.e. "The user may then be prompted to sign onto the application") [column 2 lines 32-33];
- "acquires local authentication information from the connection server" (i.e. "Each front-end server and each back-end server may store user identifiers and corresponding access privilege codes in their respective databases, rather than using a single central database to store such information") [column 3 lines 4-7];

- "the local authentication information associating the first authentication information with a predetermined authentication information and second authentication information with the predetermined authentication information" (i.e. "Each front-end server and each back-end server may store user identifiers and corresponding access privilege codes in their respective databases, rather than using a single central database to store such information") [column 3 lines 4-7];
- "stores the local authentication information" (i.e. "Each front-end server and each back-end server may store user identifiers and corresponding access privilege codes in their respective databases, rather than using a single central database to store such information") [column 3 lines 4-7];
- "receives second authentication information input by a user when the user instructs a connection request with respect to the connection server" (i.e. "The user may then be prompted to sign onto the application") [column 2 lines 32-33];
- "again calculates the first authentication information unique to the client apparatus" (i.e. "A front-end server may run the authentication process, thereby verifying the user's identification and validating the user's credentials") [column 2 lines 19-21];
- "authenticates the second authentication information and the again calculated first authentication information based on the stored local authentication information" (i.e. "a second authentication process is executed to check the authenticity of the user. This second authentication process on the back-end server") [column 2 lines 35-36];

- "if authentication is successful, encrypts the second authentication information by a first encryption method" (i.e. "The user identifier may also be encrypted as an additional security precaution") [column 11 lines 46-48];
- "transmits the encrypted second authentication information to the authentication server" (i.e. "When the user signs onto the front-end server cluster 202, the central security process 222 transmits the user login data (e.g., username and password) to the policy server 204") [column 11 lines 11-14];
- "receives, independent of the connection server, from the authentication server a connection server address of the connection server" (i.e. "Once the user is authenticated and gains access to the enterprise network (or protected resources in the enterprise network), the user's web browser may display a menu from which a service may be chosen") [column 2 lines 21-24];
- "transmits to the connection server address the second authentication information encrypted by a second encryption method" (i.e. "a second authentication process is executed to check the authenticity of the user") [column 2 lines 34-38];
- "starts communication with the connection server" (i.e. "The user may then be prompted to sign onto the application") [column 2 lines 32-33];
- "an authentication server for supplying information guiding a connection destination to the client apparatus" (i.e. "front-end server") [column 8 line 45];
- "a connection server" (i.e. "back-end content servers") [column 8 line 66].

Claim 12:

Lander discloses a connection method using a network connection system including a client apparatus, an authentication server, and a connection server comprising,

- "storing in the authentication server second connection authentication information generated by the connection server based on first connection authentication information" (i.e. "memory 106, and at least one storage device") [column 8 line 47];
- "associating the second connection authentication information with a connection server address of the connection server" (i.e. "Each front-end server and each back-end server may store user identifiers and corresponding access privilege codes in their respective databases, rather than using a single central database to store such information") [column 3 lines 4-7];
- "transmitting by the client apparatus to the authentication server a second connection authentication information generated by the client apparatus as user identification information together with a connection request" (i.e. "When the user signs onto the front-end server cluster 202, the central security process 222 transmits the user login data (e.g., username and password) to the policy server 204") [column 11 lines 11-14];
- "acquiring a client address and the user identifying information from the client apparatus when the authentication server receives the connection request from the client apparatus" (i.e. "When the user signs onto the front-end server cluster 202, the central security process 222 transmits the user login data (e.g., username and password) to the policy server 204") [column 11 lines 11-14];

- "transmitting the client address to the connection server address of the connection server when the user identification information is authenticated based on the second connection authentication information" (i.e. "Once the user is authenticated and gains access to the enterprise network (or protected resources in the enterprise network), the user's web browser may display a menu from which a service may be chosen") [column 2 lines 21-24];
- "transmitting the connection server address to the client apparatus" (i.e. "Once the user is authenticated and gains access to the enterprise network (or protected resources in the enterprise network), the user's web browser may display a menu from which a service may be chosen") [column 2 lines 21-24];
- "receiving by the client apparatus, independent of the connection server, the connection server address from the authentication server" (i.e. "Once the user is authenticated and gains access to the enterprise network (or protected resources in the enterprise network), the user's web browser may display a menu from which a service may be chosen") [column 2 lines 21-24];
- "transmitting by the client apparatus a first connection authentication information to the connection server address" (i.e. "a second authentication process is executed to check the authenticity of the user") [column 2 lines 34-38];
- "receiving by the connection server the first connection authentication information from the client address" (i.e. "The user may then be prompted to sign onto the application") [column 2 lines 32-33];

- "performing an authentication process by using the first connection authentication information transmitted from the client address" (i.e. "a second authentication process is executed to check the authenticity of the user. This second authentication process on the back-end server") [column 2 lines 35-36].

Claim Rejections - 35 USC § 103

4. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

5. Claims 2, 6, 7, 9, & 13 are rejected under 35 U.S.C. 103(a) as being unpatentable over Lander (US-7350229-B1).

Claim 2:

Lander discloses a network connection system, as in Claim 1 above, but Lander does not explicitly disclose,

- "the second connection authentication information is a message digest of the first connection authentication information," although Lander does suggest encryption of user identification/credential information, as recited below;

however, Lander does disclose,

- "The user identifier may also be encrypted as an additional security precaution" [column 11 lines 46-48];

Therefore, it would have been obvious for one of ordinary skill in the art at the time of the applicant's invention to include, "the second connection authentication information is a message digest of the first connection authentication information," in the invention as disclosed by Lander for the purposes of protecting user identification/credential information through the usage of encryption.

Claim 6:

Lander discloses a network connection system comprising,

- "a client apparatus" (i.e. "a client") [column 8 line 45];
- "a third unit for transmitting to the authentication server the first encrypted user name and the first encrypted password, which are encrypted by the first encryption method together with the connection request" (i.e. "When the user signs onto the front-end server cluster 202, the central security process 222 transmits the user login data (e.g., username and password) to the policy server 204") [column 11 lines 11-14];
- "a fourth unit for receiving the connection server address from the authentication server" (i.e. "Once the user is authenticated and gains access to the enterprise network (or protected resources in the enterprise network), the user's web browser may display a menu from which a service may be chosen") [column 2 lines 21-24];
- "transmitting to the connection server address a second encrypted user name and a second encrypted password, which are generated by encrypting using a second encryption method a user name and a password input by the user" (i.e. "a second authentication process is executed to check the authenticity of the user") [column 2 lines 34-38];
- "an authentication server" (i.e. "front-end server") [column 8 line 45];

- "a retention unit for storing a first encrypted user name and a first encrypted password, which are encrypted by a first encryption method" (i.e. "memory 106, and at least one storage device") [column 8 line 47];
- "associating a connection server address of the connection server with the first encrypted user name and first encrypted password" (i.e. "Each front-end server and each back-end server may store user identifiers and corresponding access privilege codes in their respective databases, rather than using a single central database to store such information") [column 3 lines 4-7];
- "a first unit for acquiring the first encrypted user name and the first encrypted password and a client address when the first unit receives a connection request from the client apparatus" (i.e. "When the user signs onto the front-end server cluster 202, the central security process 222 transmits the user login data (e.g., username and password) to the policy server 204") [column 11 lines 11-14];
- "the first encrypted user name and the first encrypted password being an identification for identifying a user of the client apparatus" (i.e. "The purpose of an authentication process is to determine whether the true identity of a user is that which the user presents when attempting access to the enterprise network, for example via a username, password, and credentials") [column 1 lines 55-58];

- "a second unit for transmitting the acquired client address to the connection server address associated with the user identification information" (i.e. "Once the user is authenticated and gains access to the enterprise network (or protected resources in the enterprise network), the user's web browser may display a menu from which a service may be chosen") [column 2 lines 21-24];
- "receiving from the connection server information indicating that the connection server has shifted to a connection wait state" (i.e. "The user may then be prompted to sign onto the application") [column 2 lines 32-33];
- "transmitting, independent of the connection server, the connection server address to the client apparatus" (i.e. "Once the user is authenticated and gains access to the enterprise network (or protected resources in the enterprise network), the user's web browser may display a menu from which a service may be chosen") [column 2 lines 21-24];
- "a connection server" (i.e. "back-end content servers") [column 8 line 66];

but Lander does not explicitly disclose,

- "encrypted username and encrypted password… encrypted by the first/second encryption method," although Lander does suggest encryption of user identification/credential information, as recited below;

however, Lander does disclose,

- "The user identifier may also be encrypted as an additional security precaution" [column 11 lines 46-48];

Therefore, it would have been obvious for one of ordinary skill in the art at the time of the applicant's invention to include, "encrypted username and encrypted password… encrypted by the first/second encryption method," in the invention as disclosed by Lander for the purposes of protecting user identification/credential information through the usage of encryption.

Claim 7:

Lander discloses an authentication server operating with a plurality of client apparatuses and a plurality of connection servers comprising,

- "a retention unit for storing user names and passwords, which are encrypted by a predetermined method" (i.e. "memory 106, and at least one storage device") [column 8 line 47];
- "associating each user name and each password with a connection server address of a corresponding connection server" (i.e. "Each front-end server and each back-end server may store user identifiers and corresponding access privilege codes in their respective databases, rather than using a single central database to store such information") [column 3 lines 4-7];
- "a first unit for acquiring an acquired encrypted user name, an acquired encrypted password, and an acquired client address when the first unit receives a connection request from the client apparatus" (i.e. "When the user signs onto the front-end server cluster 202, the central security process 222 transmits the user login data (e.g., username and password) to the policy server 204") [column 11 lines 11-14];

- "the encrypted user name and password being an identification information of a user of the client apparatus" (i.e. "The purpose of an authentication process is to determine whether the true identity of a user is that which the user presents when attempting access to the enterprise network, for example via a username, password, and credentials") [column 1 lines 55-58];
- "a second unit for transmitting the acquired client address to the connection server address associated with the acquired encrypted user name and password" (i.e. "Once the user is authenticated and gains access to the enterprise network (or protected resources in the enterprise network), the user's web browser may display a menu from which a service may be chosen") [column 2 lines 21-24];
- "receiving from the connection server information indicating that the connection server has shifted to a connection wait state" (i.e. "The user may then be prompted to sign onto the application") [column 2 lines 32-33];
- "transmitting, independent of the connection server, the connection server address to the client apparatus, which has issued the connection request" (i.e. "Once the user is authenticated and gains access to the enterprise network (or protected resources in the enterprise network), the user's web browser may display a menu from which a service may be chosen") [column 2 lines 21-24];

but Lander does not explicitly disclose,

- "encrypted username and encrypted password… encrypted by the first/second encryption method," although Lander does suggest encryption of user identification/credential information, as recited below;

however, Lander does disclose,

- "The user identifier may also be encrypted as an additional security precaution" [column 11 lines 46-48];

Therefore, it would have been obvious for one of ordinary skill in the art at the time of the applicant's invention to include, "encrypted username and encrypted password… encrypted by the first/second encryption method," in the invention as disclosed by Lander for the purposes of protecting user identification/credential information through the usage of encryption.

Claim 9

Lander discloses a client apparatus operating with an authentication server and a connection server comprising,

- "a connection request unit for transmitting to the authentication server a connection request and a user name and a password which are encrypted by a first encryption method" (i.e. "When the user signs onto the front-end server cluster 202, the central security process 222 transmits the user login data (e.g., username and password) to the policy server 204") [column 11 lines 11-14];
- "the connection request unit transmits to the authentication server the connection request and the user name and the password which are encrypted by the first method only when the user name and the password input by the user are authenticated by the local authentication unit" (i.e. "a second authentication process is executed to check the authenticity of the user") [column 2 lines 34-38];

- "a receiving unit for receiving, independent of the connection server, a connection server address from the authentication server" (i.e. "Once the user is authenticated and gains access to the enterprise network (or protected resources in the enterprise network), the user's web browser may display a menu from which a service may be chosen") [column 2 lines 21-24];
- "encrypting by a second encryption method the user name and the password input by a user" (i.e. "The user identifier may also be encrypted as an additional security precaution") [column 11 lines 46-48];
- "a transmitting unit for transmitting the encrypted user name and password to the connection server address" (i.e. "a second authentication process is executed to check the authenticity of the user") [column 2 lines 34-38];
- "a retention unit for storing local authentication information, which is previously supplied from the connection server" (i.e. "memory 106, and at least one storage device") [column 8 line 47];
- "the local authentication information associating unique information of the client apparatus with at least one of a user name and a password previously provided to the connection server" (i.e. "Each front-end server and each back-end server may store user identifiers and corresponding access privilege codes in their respective databases, rather than using a single central database to store such information") [column 3 lines 4-7];

- "a local authentication unit for generating the unique information upon receiving a user name and a password input by the user" (i.e. "The purpose of an authentication process is to determine whether the true identity of a user is that which the user presents when attempting access to the enterprise network, for example via a username, password, and credentials") [column 1 lines 55-58];
- "authenticating the user name and the password input by the user by judging based on the local authentication information whether or not at least one of the user name and the password input by the user is associated with the unique information" (i.e. "a second authentication process is executed to check the authenticity of the user. This second authentication process on the back-end server") [column 2 lines 35-36];

but Lander does not explicitly disclose,

- "encrypted username and encrypted password…encrypted by the first/second encryption method," although Lander does suggest encryption of user identification/credential information, as recited below;

however, Lander does disclose,

- "The user identifier may also be encrypted as an additional security precaution" [column 11 lines 46-48];

Therefore, it would have been obvious for one of ordinary skill in the art at the time of the applicant's invention to include, "encrypted username and encrypted password…encrypted by the first/second encryption method," in the invention as disclosed by Lander for the purposes of protecting user identification/credential information through the usage of encryption.

Claim 13

Lander discloses a connection method using a network connection system including a client apparatus, an authentication server, and a connection server comprising,

- "storing by the authentication server a user name and a password which are encrypted by a first encryption method" (i.e. "memory 106, and at least one storage device") [column 8 line 47];
- "associating the encrypted user name and the encrypted password with a connection server address of the connection server" (i.e. "Each front-end server and each back-end server may store user identifiers and corresponding access privilege codes in their respective databases, rather than using a single central database to store such information") [column 3 lines 4-7];
- "transmitting by the client apparatus to the authentication server a connection request and the user name and the password which are encrypted by the first encryption method" (i.e. "When the user signs onto the front-end server cluster 202, the central security process 222 transmits the user login data (e.g., username and password) to the policy server 204") [column 11 lines 11-14];
- "receiving by the authentication server the connection request from the client apparatus" (i.e. "When the user signs onto the front-end server cluster 202, the central security process 222 transmits the user login data (e.g., username and password) to the policy server 204") [column 11 lines 11-14];

- "acquiring a client address of the client apparatus and the user name and the password, which are encrypted by the first encryption method, as information identifying a user of the client apparatus" (i.e. "When the user signs onto the front-end server cluster 202, the central security process 222 transmits the user login data (e.g., username and password) to the policy server 204") [column 11 lines 11-14];
- "transmitting the client address to the connection server address" (i.e. "Once the user is authenticated and gains access to the enterprise network (or protected resources in the enterprise network), the user's web browser may display a menu from which a service may be chosen") [column 2 lines 21-24];
- "receiving by the connection server the client address" (i.e. "Once the user is authenticated and gains access to the enterprise network (or protected resources in the enterprise network), the user's web browser may display a menu from which a service may be chosen") [column 2 lines 21-24];
- "allowing communication from the client apparatus" (i.e. "The user may then be prompted to sign onto the application") [column 2 lines 32-33];
- "transmitting to the authentication server information indicating that the connection server has shifted to a connection wait state in which the connection server allows communication from the address of the client apparatus for a predetermined period" (i.e. "The user may then be prompted to sign onto the application") [column 2 lines 32-33];
- "encrypting using a second encryption method a user name and a password input by a user" (i.e. "The user identifier may also be encrypted as an additional security precaution") [column 11 lines 46-48];

- "transmitting to the connection server address the user name and the password which are encrypted by the second encryption method" (i.e. "a second authentication process is executed to check the authenticity of the user") [column 2 lines 34-38];
- "performing an authentication process by using the user name and the password which are encrypted by the second encryption method and are received by the connection server from the client apparatus" (i.e. "a second authentication process is executed to check the authenticity of the user. This second authentication process on the back-end server") [column 2 lines 35-36];

but Lander does not explicitly disclose,

- "encrypted username and encrypted password…encrypted by the first/second encryption method," although Lander does suggest encryption of user identification/credential information, as recited below;

however, Lander does disclose,

- "The user identifier may also be encrypted as an additional security precaution" [column 11 lines 46-48];

Therefore, it would have been obvious for one of ordinary skill in the art at the time of the applicant's invention to include, "encrypted username and encrypted password…encrypted by the first/second encryption method," in the invention as disclosed by Lander for the purposes of protecting user identification/credential information through the usage of encryption.

Response to Arguments

6. Applicant's arguments with respect to claims 1-3, 5-7, & 9-13 have been considered but are moot in view of the new ground(s) of rejection as necessitated by the applicant's amendments and with further search and consideration of their limitations in light of the applicant's remarks.

Conclusion

7. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Examiner Oscar Louie whose telephone number is 571-270-1684. The examiner can normally be reached Monday through Thursday from 7:30 AM to 4:00 PM.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Nasser Moazzami, can be reached at 571-272-4195. The fax phone number for Formal or Official faxes to Technology Center 2100 is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private

PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

OAL
05/06/2008

/Brandon S Hoffman/
Primary Examiner, Art Unit 2136